Hearing on "Cyber Attack: Is the Government Safe?"

SENATOR DANIEL K. AKAKA

Senate Governmental Affairs Committee
March 2, 2000

Thank you Mr. Chairman and Senator Lieberman for providing the opportunity to discuss cybersecurity. In this new age of information warfare, no issue is of more vital importance to our security.

A cyber attack against our national information infrastructure would affect the integrity of our telecommunications, energy, banking and finances, transportation, water systems, and emergency services. As the Ranking Member of the Subcommittee on International Security, Proliferation, and Federal Services, I applaud all efforts to call attention to this issue. It is one in which the subcommittee has also been involved . The Chairman and Ranking Member deserve great credit for the effort that they have made to heighten awareness of the threat while proposing methods to counter the threat.

Computer hacking can no longer be labeled benign mischief. Once, those who gained unauthorized access to government and private sector computer networks were heralded as technical icons, whose exploits were lionized by the popular media. That is not the reality any more. Now hacking is a federal crime at the very least - at the worst, an international act of aggression. As Deputy Secretary of Defense John Hambre has stated, "We are at war - right now. We are in a cyber war."

Total losses from cyber fraud, including loss of service, recovery, and restoration costs, are estimated to be in the hundreds of millions of dollars. We now know that hostile countries have, or are developing, the capability to engage in overt and covert information warfare.

Last year alone there were more than 20,000 cyber attacks on Department of Defense networks alone. Astonishingly, we do not know who was behind the majority of those attacks.

In 1998, during a period of increased tensions with Iraq over United Nations weapons inspections, over 500 U.S. military, civilian government, and private sector computer systems were attacked. What was first thought to be a sophisticated Iraqi cyber attack proved to be a rather unsophisticated, yet highly effective attack by two juveniles from California with the cooperation of several individuals in Israel.

Last month, cyber-based denial of service attacks had a dramatic and immediate impact on many Americans and resulted in the loss of millions of dollars when several large e-commerce sites were shut down for several hours.

Just recently a student at a major university was arrested and charged with hacking into federal government computers at the National Aeronautics and Space Administration (NASA) and the Department of Defense where he was able to read, delete, and alter protected files and intercept and save log-in names.

Clearly, cybercrime has become a pervasive problem. And it is getting worse. According to FBI Director Louis Freeh, cybercrime is one of the fastest evolving areas of criminal behavior and a significant threat to our national and economic security. The escalation of cybercrime is rapidly overwhelming our current capability to respond.

Current technology has thus far failed to provide adequate safeguards for critical infrastructure networks. The Internet is international, knowing no boundaries and no ownership. Any attempt to stifle its growth and development would be counter productive to the economic interests of America. A variety of easy to use sophisticated hacker tools are freely available on the Internet, available for use by anyone in the world with an inclination to mount a cyber attack.

Today, the United States has little ability to detect or recognize a cyber attack against either government or private sector infrastructures and even less capability to react. Nevertheless, we must, through cooperative public and private sector efforts, develop adequate defensive technologies to neutralize threats. Without new defenses, it is likely that attacks will occur with greater frequency, do more damage, and be more difficult to detect and counter.

In January 2000, President Clinton unveiled his "National Plan for Information Systems Protection," which proposes critically needed infrastructure improvements with milestones for implementation. This multifaceted plan promotes an unprecedented level of public/private cooperation, and proposes 10 programs to assess vulnerabilities, and significantly enhance capabilities to deter, detect, and effectively respond to hacking incidents. It also calls for vital research and educational enhancements to train adequate numbers of desperately needed information security specialists and sustain their perishable skills.

Our continued leadership and prosperity in the global economy may well hinge on our national commitment to act as leaders in bringing information assurance to the global information environment we have helped to create. I commend the Chairman and Ranking Member for their leadership in calling attention to this particularly insidious problem by their introduction of S.1993, the Government Information Security Act. I welcome our witnesses, and look forward to hearing their testimony today.